UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/961,380	09/25/2001	Ned M. Smith	P 282600 P11801	5485

27496 7590 04/05/2005

PILLSBURY WINTHROP LLP
725 S. FIGUEROA STREET
SUITE 2800
LOS ANGELES, CA 90017

EXAMINER	
WILLIAMS, JEFFERY L	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/961,380	SMITH ET AL.
	Examiner	Art Unit
	Jeffery Williams	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 23 February 2004.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-29 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 11 February 2002 is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 317, 680, 740, 750, 760, and 770. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

Claim 4 is objected to because of the following informalities: lines 3 and 12 contain grammatical errors. Appropriate correction is required.

Claim Rejections - 35 USC § 112

Claim 4 is rejected as failing to define the invention in the manner required by 35 U.S.C. 112, second paragraph.

The claim must be in one sentence form only.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 – 3, 6, 7, 10, 11, 14, 15, and 18 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier, Applied Cryptography.

Regarding claim 1, Schneier discloses a method comprising:

establishing a physical channel between a sender and a receiver (Schneier, pg. 2, par. 1; pgs. 22,23; pgs. 576, 577). As disclosed by Schneier, the disclosed method deals with computer cryptography. The method is implemented on a computer network with hardware such as PCs or VAXs, and is a communication protocol between senders and receivers on the computer network. Alice and Bob represent the network senders and receivers. Thus, Schneier discloses a physical channel between a sender and receiver.

sending, from the sender to the receiver, data through a data channel (Schneier, pg. 576, protocol steps 2,3). Data is sent from a sender to a receiver, thus a data channel exists.

receiving, at the receiver, the data (Schneier, pg. 576, protocol steps 3,4).

and verifying, between the receiver and the sender via the physical channel, that the data is from the sender (Schneier, pg. 576, protocol steps 3-5).

Regarding claim 2, Schneier discloses wherein that data includes:

a key; and a nonce (Schneier, pg. 576, protocol steps 1-3).

Regarding claim 3, Schneier discloses wherein the verifying comprises *performing receiver-initiated verification* (Schneier, pg. 577, protocol steps 9-11).

Regarding claims 6, 7, 10, and 11, they recite the limitations found in claims 1 –3, and are rejected by the same rational.

Regarding claim 14, it is the system claim corresponding to the method of claim 1, and is rejected by the same rational.

Regarding claim 15, Schneier discloses:

an information generation mechanism for generating the data (Schneier, pg. 576, protocol steps 1, 2).

a transmitter for transmitting the data to the receiver via the data channel (Schneier, pg. 576, protocol step 3).

a first verification mechanism for verifying, via the physical channel, that the data received by the receiver is from the sender (Schneier, pg. 577, protocol steps 16).

Regarding claim 18, it recites the same limitations as claim 15, and is rejected by the same rational.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 5, 8, 9, 12, 13, 16, 17, 19 - 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, Applied Cryptography.

Regarding claim 4, Schneier discloses wherein the performing receiver-initiated verification comprises *repeating, by the receiver upon receiving the data, the nonce to* *generate a repeating nonce* (Schneier, pg. 577, protocol step 10). The sender repeats the nonce R_a. He further discloses *perceiving, by the sender, the repeating nonce* (Schneier, pg. 577, protocol step 16), and *verifying the perceived repeating nonce is semantically related to the nonce sent* (Schneier, pg. 577, protocol step 16).

While Schneier discloses acknowledging to the receiver that the verification message was successful (Schneier, pg. 577, protocol step 17), he does not disclose that this is based upon *if the perceived repeating nonce is verified.* However, in step 16, the sender checks that the received nonce R_a is equal to the sent nonce R_a, thus verifying that the receiver had successfully received the sender's message containing the key. Steps 1 – 19 of Schneier's authentication protocol demonstrate an ordered progression of communications toward the goal of establishing secure and authenticated communication link. It is obvious, based upon logical reasoning, that the sender's acknowledgement message in step 17, is in view of the verification in the preceding step 16. In like manner, it is logical to conclude that the verification in step 16, is performed for a purpose, and should step 16 fail, the sender would not purpose to continue in the ordered progression of communications to step 17. Thus, it would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to recognize that the disclosure of Schneier implies the acknowledgement to the receiver that the verification message was successful *if the perceived repeating nonce is verified*, because it is logical to conclude that if the repeating nonce were not verified, step 17 would not be performed.

Regarding claim 5, the qualification of Schneier discloses *sending, from the sender to the receiver, if the verifying is successful, a signed message* (Schneier, pg. 577, protocol step 17). The qualification of Schneier further discloses, *verifying the signature in the signed message using the stored key* (Schneier, pg. 577, protocol step 18). Notice, the key obtained by the receiver in step 4 is employed at a later time by the receiver in step 18. Therefore, Schneier implies using the stored key.

The qualification of Schneier does not disclose that the key is stored by the receiver if *the verifying is successful.* However, it is logical that a receiver, desiring a verified key for communication, would proceed to store (instead of discarding) the key in memory for future use if it were verified. Therefore, it would have been obvious to one of ordinary skill in the art, based upon logical reasoning, to recognize that the qualification of Schneier implies storing the key if it were verified, because a receiver desiring to employ a verified key would store the verified key for future use.

Regarding claims 8, 9, 12, and 13, they recite the limitations found in claims 4 and 5, and are rejected by the same rational.

Regarding claim 16, the qualification of Schneier discloses:

a transmission receiver for intercepting the data, sent from the sender through the data channel (Schneier, pg. 576, protocol steps 3,4). As explained in claim 1, Alice and Bob represent senders and receivers on a computer network. Thus, Schneier, discloses a transmission receiver (Bob).

a second verification mechanism for verifying, via the physical channel and cooperating with the first verification mechanism in the sender, that the data received is from the sender (Schneier, pg. 576, protocol steps 4-8).

and a key storage for storing a key included in the received data, if the verifying is successful (Schneier, pgs. 576, 577, protocol steps 4-8).

Regarding claim 17, the qualification of Schneier discloses:

the sender further comprising a signed message generation mechanism for generating a signed message to be sent, after the verifying, to the receiver through the transmitter, the signed message including a signature of the sender (Schneier, pgs. 576, 577, protocol steps 1, 2, 3, 17). Schneier discloses that the sender comprises the ability to generate data and construct a message, the message bearing the signature of the sender. Thus, Schneier discloses that

the receiver further comprising a signature verification mechanism for verifying, upon receiving the signed message, the signature of the sender received through the transmission receiver.

Regarding claim 19, it recites the limitations found in claim 8, and is rejected by the same rational.

Regarding claims 20 and 21, they recite the same limitations found in claims 17 and 16, and are rejected by the same rational.

Regarding claim 22, the qualification of Schneier discloses a receiver-initiated verification mechanism for performing a receiver-initiated verification, comprising:

an nonce repeater for generating a repeating nonce using the nonce contained in the data sent from the sender (Schneier, pg. 577, protocol step 10).

and an acknowledgement perceiver for perceiving an acknowledgement from the sender that acknowledges that the repeating nonce is same as the nonce contained in the data (Schneier, pg. 577, protocol steps 18, 19).

Regarding claim 23, the qualification of Schneier discloses *a signature verification mechanism for verifying the signature of the sender contained in a signed message, sent from the sender after the verifying and received by the receiver through the transmission receiver* (Schneier, pg. 577, protocol step 18).

Regarding claim 24, the qualification of Schneier does not disclose a computer-readable medium encoded with a program. However, it is obvious that the sending and receiving computers of data on the computer network disclosed by Schneier would comprise a medium encoded with computer instructions. Thus, it would have been obvious to one of ordinary skill in the art to recognize that the qualification of Schneier would contain computer readable medium encoded with a program because a network of operating computers could not operate without computer instructions embodied in a medium.

Therefore, the qualification of Schneier discloses:

sending, from a sender to a receiver, data through a data channel (Schneier, pg. 576, protocol step 3).

receiving, at receiver, the data (Schneier, pg. 576, protocol steps 3,4).

storing, by the receiver, a part of the data as a stored key, after verifying, via a physical channel established between the sender and the receiver, that the data received by the receiver is from the sender (Schneier, pg. 576, protocol steps 4,5,10, and 18).

sending, from the sender to the receiver, if the verification is successful, a signed message containing a signature of the sender (Schneier, pg. 577, protocol steps 16, 17).

receiving, at the receiver, the signed message (Schneier, pg. 577, protocol steps 17, 18).

and authenticating the signature in the signed message using the stored key (Schneier, pg. 577, protocol step 18).

Regarding claim 25, the qualification of Schneier discloses:

performing receiver-initiated verification via the physical channel (Schneier, pgs. 576, 577, protocol steps 1-19).

Regarding claims 26 – 29, they recite the same limitations found in claims 24 and 25, and are rejected by the same rational.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

Jeffery Williams
Art Unit: 2137
(571) 272-7965